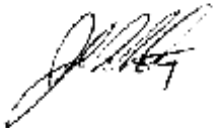




U.S. DEPARTMENT OF COMMERCE
National Oceanic and Atmospheric Administration
NATIONAL WEATHER SERVICE
Silver Spring, Md. 20910

MEMORANDUM FOR: All NWS Regional Headquarters, Regional
Maintenance Specialists, Electronic Systems
Analysts, and Electronics Technicians
[Engineering Handbook (EHB)-13, Series II
distribution]

FROM: W/OPS1 - John McNulty 

SUBJECT: Transmittal Memorandum for EHB-13, Series
II, Issuance 00-21

1. Material Transmitted:

Advanced Weather Interactive Processing System (AWIPS),
Section 2.1, AWIPS System Security Note 1, LDAD Security
Patch Bundle. Patch number P432_PRC_A100083.

2. Summary:

AWIPS System Security Note 1 provides instructions for
installing a software patch that improves the Local Data
Acquisition and Dissemination security.

3. Effect on Other Instructions:

None.



AWIPS SYSTEM SECURITY NOTE 1 (for Electronics Systems Analysts)

Engineering Division

W/OSO321: FJZ

SUBJECT : LDAD Security Patch Bundle

PURPOSE : To provide instructions on improving Local Data Acquisition and Dissemination (LDAD) security. Patch number P432_PRC_A100083

VERIFICATION STATEMENT : These procedures were verified at the Burlington, VT (BTV) and Bismarck, ND (BIS) Weather Forecast Offices

SECURITY LEVEL : root

BACKGROUND

The Advanced Weather Interactive Processing System (AWIPS) program office tasked the Aerospace Corporation to perform a vulnerability assessment of the AWIPS security features. The analysis focused on the interface between the AWIPS wide area network (WAN) and LDAD. Since disclosure of AWIPS data is not an issue, the vulnerability test was carried out to assess system integrity, data integrity, and the possibility of disrupting service. These instructions and associated patch are a result of the penetration test analysis and require immediate action.

The patch will perform the following function:

- ⌄ Upgrade/update the LDAD COTS security package.
- ⌄ Increase restrictions to the AWIPS firewall rule set.
- ⌄ Eliminate the "setuid" script from the LDAD server.

PROCEDURE

A. LDAD Security Patch Installation Procedure

1. At a workstation, log in to ds1 as **root** and perform a remote log in to ls1 by typing:

```
rlogin ls1
```

2. Ensure the “/var” directory has at least 10 MB of available disk space. From the root directory type:

```
du -s /var
```

The number should be more than 10000. If not, delete/backup any unnecessary files from the “/var” directory.

3. Change to the “/var” directory by typing:

```
cd /var
```

4. Check for the existence of the “tmp” directory by typing:

```
ll
```

5. If the “tmp” directory does not exist, create it by typing:

```
mkdir tmp
```

6. Exit ls1 and log back into ds1 by typing:

```
exit
```

7. Change to the “/awips” directory by typing:

```
cd /awips
```

8. Check for the existence of the “tmp” subdirectory by typing:

```
ll
```

9. If the “tmp” directory does not exist, create it by typing:

```
mkdir tmp
```

10. Change to the “tmp” directory by typing:

```
cd tmp
```

11. Connect to the NOAA1 ftp server by typing:

```
ftp 165.92.30.15
```

12. Once connected, log in as **ftp** user with the **4Awips!** password.

13. Get the “ldadPatch.tar” file by typing:

```
binary
hash
cd /pub
get ldadPatch.tar
bye
```

14. From ds1, copy the “ldadPatch.tar” file to the ls1 “/var/tmp” directory by typing:

```
rcp ldadPatch.tar ls1:/var/tmp
```

15. At the Xyplex system console, configure the system console to the LDAD side.

16. From the system console log in to ls1 as **root** and change to the “/var/tmp” directory by typing:

```
cd /var/tmp
```

17. Unbundle the “ldadPatch.tar” file to obtain the “README.firewall,” “README.patches,” and bundled “ldad.tar” files by typing:

```
tar xvf ldadPatch.tar
```

The 3 unbundled files contain the following information:

- C “README.firewall” contains instructions for configuring firewall ports 15007 through 15008.
- C “README.patches” contains instructions for installing the security patches on the LDAD server.
- C “ldad.tar” is a tar file containing a README, scripts, and the tar files associated with the LDAD security patch.

18. Unbundle, then delete the “ldad.tar” file by typing:

```
tar xvf ldad.tar
rm ldad.tar
```

This will yield the following 3 files:

```
C  ldad_patches.tar
C  install_ldad_patches
C  postinstall_ldad_patches
```

19. Run the script to install the patch by typing:

```
script -a /var/tmp/install_ldad_patches.out
./install_ldad_patches
```

NOTE: 1. Disregard any displayed warnings while the patch is executing.

2. The script will query for the presence of a critical patch. If the patch is not present, the script will install the patch and reboot the LDAD server. If the patch is already installed, the LDAD server will not reboot.

20. Type **exit** to exit the script and type **exit** again to log out of ls1.
21. At a workstation, log in to ds1 as **root**, then remote log in to ls1 by typing:

```
rlogin ls1
```

22. Grep for the script process and kill if necessary by typing:

```
ps -ef | grep script
kill -9 <process number>
```

23. Update the patch log file by typing:

```
cd /var/tmp
script -a /var/tmp/postinstall_ldad_patches.out
./postinstall_ldad_patches
```

24. Enter name and phone number when prompted.
25. Type **exit** to exit the script.
26. Type **exit** to return to ds1.

27. To view the “/etc/host” file, type: .

```
more /ect/host
```

28. Verify the third octal of the local AWIPS IP address. This will be used for the next procedure

This concludes the LDAD security patch installation procedure.

B. Firewall Configuration Procedure

The following procedure gives instructions on modifying the LDAD firewall ruleset to increase access control connection between the LDAD server and AWIPS.

1. At the Xyplex system console, configure the system console to the AWIPS side.
2. At the system console, log into the LDAD firewall as **root** by typing:

```
XYPLEX > c xyplex1:5800
```

3. After the following line is displayed, press **5 Enter**

```
XYPLEX-010-Session 1 to XYPLEX1:5800 established
```

4. Continue by logging in as **root** user and entering the password by typing:

```
login: root
```

```
Password: xxxxxxxx
```

5. Start the gauntlet-admin program by typing:

```
gauntlet-admin
```

6. Using the down arrow key, cursor down to select the following options:

```
Optional System Configuration 5 Enter
```

```
Packet Screen Configuration 5 Enter
```

```
Edit Forward Rulesets 5 Enter
```

7. Using the down arrow key, cursor to rule #1 and press **5 Enter** to access the editor.
 - a. Using the tab key, cursor down to the Destination Address field.
 - (1) For example, the Destination Address may look similar to:

165.92.0.0
 - (2) Use the backspace or shift-del keys to change the 3rd octet (0) to the local AWIPS subnet.
 - b. Tab to the Destination Address Mask field.
 - (1) For example, the Destination Address Mask may look similar to:

255.255.0.0
 - (2) Use the backspace or shift-del keys to change the mask to 255.255.255.128
 - (3) Tab to the menu options on the bottom of the screen, then arrow down to Save these changes; press **5 Enter**.
8. Using the down arrow key, cursor to rule #2 and press **5 Enter** to access the editor.
 - a. Tab to the Source Address field.
 - (1) For example, the Source Address may look similar to:

165.92.0.0
 - (2) Use the backspace or shift-del keys to change the 3rd octet (0) to the local AWIPS subnet.
 - b. Tab to the Source Address Mask field.
 - (1) For example, the Source Address Mask may look similar to:

255.255.0.128
 - (2) Use the backspace or shift-del keys to change the mask to 255.255.255.128.
 - (3) Tab to the menu options on the bottom of the screen, then arrow down to Save these changes; press **5 Enter**.

9. Using the down arrow key, cursor to rule #3 and press **5 Enter** to access the editor.
 - a. Tab to the Source Address field.
 - (1) For example, the Source Address may look similar to:

165.92.0.0
 - (2) Use the backspace or shift-del keys to change the 3rd octet (0) to the local AWIPS subnet.
 - b. Tab to the Source Address Mask field.
 - (1) For example the Source Address Mask may look similar to:

255.255.0.0
 - (2) Use the backspace or shift-del keys to change the mask to 255.255.255.128.
 - (3) Tab to the menu options on the bottom of the screen, then arrow down to Save these changes; press **5 Enter**.
10. Using the down arrow key, cursor to rule #4 and press **5 Enter** to access the editor.
 - a. Tab to the Destination Address field.
 - (1) For example, the Destination Address may look similar to:

165.92.0.0
 - (2) Use the backspace or shift-del keys to change the 3rd octet (0) to the local AWIPS subnet.
 - b. Tab to the Destination Address Mask field.
 - (1) For example the Source Address Mask may look similar to:

255.255.0.0
 - (2) Use the backspace or shift-del keys to change the mask to 255.255.255.128.
 - (3) Tab to the menu options on the bottom of the screen, then arrow down to Save these changes; press **5 Enter**.

11. From the Packet Filter Rule Editor - Forward ruleset menu, use the tab key to move the cursor to bottom of screen and arrow down to the Save and Exit and press **5 Enter**.
12. From the Optional Configuration Menu, tab to Return to Previous Menu. Then press **5 Enter**
13. From the Gauntlet Internet Firewall Main Management Menu, tab to Update Configuration Menu and press **5 Enter**.
14. Select Quit, and Update Configuration Database. Press **5 Enter**.
15. Type **y** when prompted for Rebuild system configuration files?. Then press **5 Enter** to resume.
16. At the firewall prompt, run the "updt_table" script to update the "netperm-table" by typing:


```
cd /etc/scripts  
./updt_table
```
17. To effect the changes reboot the firewall by typing:


```
shutdown -r now
```
18. The reboot will bring up the Xyplex terminal server menu. Logout of the terminal server.

This completes the firewall configuration procedure.

REPORTING MODIFICATION

Report the completed modification on a WS Form A-26, Maintenance Record according to instructions in Engineering Handbook 4 (EHB-4), part 2, and appendix H. A sample A-26 form is attached. As an additional guide, use the information in the table below.

Block #	Block Type	Information
5	Description	Installed LDAD security patch I.A.W. AWIPS System Security Note 1
7	Equipment Code	AWIPS
8	Serial Number	001
15	Comments	Update AWIPS system software with LDAD Security Patch (number P432_PRC_A100083, I.A.W. Security Note 1
17a	Mod. No.	SS1

TECHNICAL SUPPORT

For questions or problems regarding this procedure, call the NCF at 301-713-9344.



John McNulty
Chief, Maintenance, Logistics, and Acquisition Division

Attachment A

WS FORM A-26 (4/94)		WS FORM A-26 (4/94)				U.S. DEPARTMENT OF COMMERCE NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION NATIONAL WEATHER SERVICE				Document Number G 49978			
ENGINEERING MANAGEMENT REPORTING SYSTEM MAINTENANCE RECORD													
General Information		1. Open Date 11 / 20 / 00		Time 0900		2. Initials JMM		3. Response Priority (check one) <input type="radio"/> Immediate <input type="radio"/> Low <input type="radio"/> Routine <input checked="" type="radio"/> Not Applicable		4. Close Date 11 / 20 / 00		Time 1000	
5. Description Installed LDAD security patch I.A.W. AWIPS System Security Note 1													
Equipment Information		6. Station ID CTP		7. Equipment Code AWIPS		8. Serial Number 001		9. TM M		10. AT M		11. How Mal. 999	
1 2. EQUIPMENT OPERATIONAL STATUS TIMES		a. Fully Operational <input type="text"/>		b. Logistics Delay <input type="text"/>		Partly Operational		c. All Other <input type="text"/>		d. Logistics Delay <input type="text"/>		Not Operational e. All Other <input type="text"/>	
13. Parts Failure Information										14. Work Load Information			
Block #	a. ASN	b. NSN	c. TM	d. AT	e. How Mal.	f. Qty.	g. Maint. Hrs.	Type	Staff Hrs.				
1								a. Routine					
2								b. Non-routine					
3								c. Travel					
4								d. Misc.	1:00				
5								e. Overtime					
Miscellaneous Information		15. Maintenance Comments Update AWIPS System software with LDAD Security Patch (number P432_PRC_A100083), I.A.W. Security Note 1								16. Initials JMM			
17. SPECIAL PURPOSE REPORTING		a. Mod. No. SS1		b. Mod./Act./Deact.Date 11/20/00		c.		d.		e.			
18. CONFIGURATION MGMT. REPORTING (use as directed)		ASN		Vendor Part Number (New Part)		Serial Number (Old Part)		Serial Number (New Part)					